IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

JASON WILLIAMS, Plaintiff, v. AT&T MOBILITY LLC, Defendant.	Case No. 5:19-cv-00475-BO **[PROPOSED] JOINT PRETRIAL ORDER**

Date of Conference: February 14, 2023

Appearances: For Plaintiff Jason Williams:

Christopher LaVigne, Withers Bergman LLP, New York, New York
Joseph Gallo, Withers Bergman LLP, New York, New York
Dhamian Blue, Blue LLP, Raleigh, North Carolina

For Defendant AT&T Mobility LLC:

Joseph S. Dowdy, Kilpatrick Townsend, Raleigh, North Carolina
Nancy L. Stagg, Kilpatrick Townsend, San Diego, California
S. Mark Henkle, Kilpatrick Townsend & Stockton, Winston-Salem, North Carolina

I. STIPULATIONS

A. Parties, Jurisdiction, and Witnesses

1. All parties are properly before the court.

2. The Court has jurisdiction over the parties and the subject matter.

3. All the parties have been correctly designated.

4. There is no question as to misjoinder or nonjoinder of the parties.

5. Plaintiff will appear for trial and will make Jameson Lopp available to testify at trial without the need for trial subpoenas, for either party to call as

witnesses. Defendant will make Ray Hill, Valerie Scheder, Robert Arno, Ryan Garlick, Richard Sanders, and Stephen Mott available to testify at trial without the need for trial subpoenas, for either party to call as witnesses.

B. Factual Stipulations

1. Plaintiff Jason Williams is a natural person, who was at all relevant times a resident of North Carolina.

2. Defendant AT&T Mobility, LLC ("AT&T") is a Delaware limited liability corporation with its principal office or place of business in Brookhaven, Georgia. AT&T provides telecommunications services in the United States, Puerto Rico, and the U.S. Virgin Islands.

3. AT&T is a common carrier or carrier within the meaning of the Federal Communications Act, only for the purposes of Mr. Williams' claims in this lawsuit under 47 USC § 222.

4. Mr. Williams is a former customer of AT&T. In or around 2000, Mr. Williams purchased a wireless cell phone plan from AT&T in Raleigh, Wake County, North Carolina. Mr. Williams was an active, paying AT&T wireless subscriber until approximately February 6, 2019.

5. There were six SIM changes performed on Mr. Williams' AT&T account between November 5, 2018, and February 6, 2019.

II. CONTENTIONS

A. Plaintiff's Factual Contentions. Plaintiff intends to prove the following contested facts at trial:

1. Plaintiff Jason Williams is a natural person, who was at all relevant times a resident of North Carolina. He currently resides in Raleigh, Wake County, North Carolina with his wife and three daughters.

2. As of August 2019, AT&T had 130 stores in North Carolina, including 11 stores in Raleigh, North Carolina.

3. Mr. Williams is a co-founder and partner of an asset management company that invests in blockchain technology and digital assets.

4. Apollo Kids Mining, LLC ("Apollo") is an active Limited Liability Company registered in Delaware. Mr. Williams is the founder, and sole member of Apollo, which formally discontinued its large-scale bitcoin mining operation in May 2019, due to the effects of the SIM-swap attacks against Mr. Williams.

5. A SIM ("subscriber identification module") card is a small, removable chip that allows a cell phone to communicate with the wireless service provider, or "carrier," and allows the carrier to know which subscriber account is associated with that phone.

6. The connection between the phone and the SIM card is made through the carrier, which associates each SIM card with the physical phone's IMEI ("international mobile equipment identity"), which is akin to the phone's serial number.

7. SIM cards can also store a limited amount of account data, including contacts, text messages, and carrier information, and that data can help identify the subscriber.

8. The SIM card associated with a wireless phone can be changed, or "swapped." When done properly, with the customer's authorization, this allows customers to move their wireless number from one cell phone to another and to continue accessing the carrier network when they switch cell phones.

9. For a SIM card change to be effective, the carrier – through its employees, customer service personnel, and other agents – must authenticate the request and make the requested change.

10. Between November 5, 2018, and February 6, 2019, AT&T allowed its employees, contractors, and agents to conduct SIM swaps for its customers either remotely, over the phone, or in-person, in its retail stores.

11. A fraudulent SIM swap typically involves the unauthorized transfer of the customer's phone number to a SIM card that is inside a wireless device in possession of a person besides the customer.

12. Following a fraudulent and unauthorized SIM swap, the new person gains the ability to use the customer's phone number for calls and text messages. Meanwhile, the customer's phone loses its connection to the carrier network, rendering it unable to make phone calls or text messages.

13. In September 2017, AT&T's Vice President of Security Platforms published an article on AT&T's "Cyber Aware" blog about unauthorized SIM swaps.

14. On May 5, 2017, AT&T released a video concerning the threat of company insiders selling customer information and access, citing a survey

showing that a significant number of employees would deliberately sell corporate log-ons or sell corporate data for small amounts of money.

15. As of the date of the complaint in this action, AT&T's website prominently stated: "Your security is our top priority. We're bringing together all our security features to keep you protected."

16. As of the date of the complaint in this action, AT&T published a Privacy Policy in which it represents that it will protect customers' privacy and keep their personal information safe.

17. As of the date of the complaint in this action, AT&T's Privacy Policy stated that it does not sell, trade, or share a customer's CPNI, with anyone outside the AT&T family of companies, or AT&T's authorize agents, unless required by law.

18. As of the date of the complaint in this action, AT&T's Privacy Policy further states that it "uses technology and security features, and strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI. It is your right and our duty under federal law to protect the confidentiality of your CPNI."

19. As of the date of the complaint in this action, AT&T recognized the risks that arise when a cell phone is compromised, stating, "Our phones are mini-computers, and with so much personal data on our phones today, it's also important to secure our mobile devices."

20. AT&T released an advertising video, in which its employees discuss "threat hunting" which they describe as "an active threat analysis where you're

actually thinking about your adversary." In the video, the employees state that it is "important" and "something [AT&T has] been doing for a long time." They state that [AT&T] thinks about "what would a hacker want to do, where would a hacker go to get my data, what are some of the points on my network that are most vulnerable, or where is the data flow that is potentially going to be a leakage" and state that "having threat hunting as part of a proactive continuous program, integrating with existing security measures, will help [you] stay ahead of the threats." AT&T's advertising video further stated that these practices could help identify "insider threats"—employees within the company.

21. In 2016, AT&T implemented a waterfall security protocol in order to authenticate and effectuate customer SIM card changes, in which AT&T personnel were supposedly required to go through a proscribed series of verification steps before complying with requests for SIM card changes, in order to prevent unauthorized SIM Swaps.

22. This authentication waterfall security protocol was in place when Mr. Williams was an AT&T customer, including between November 5, 2018, and February 6, 2019.

23. FCC Rules, set forth at 47 C.F.R. § 64.2001 et seq., and the FCA restrict AT&T's use and disclosure of CPNI, and require that AT&T take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. FCC Rules and the FCA require that AT&T notify the FBI and consumers when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

24. Between November 5, 2018, and February 6, 2019, six unauthorized SIM swaps were performed on Mr. Williams' AT&T wireless telephone account.

25. These unauthorized SIM swaps were the result of AT&T's decisions and the negligence of AT&T employees and agents and/or the knowing, deliberate assistance of AT&T employees and agents. These unauthorized SIM swaps were conducted despite AT&T's customer account authentication and security efforts, which AT&T knew or should have known were inadequate to protect customers from such unauthorized SIM swaps.

26. In each of these SIM swap attacks, AT&T used and/or disclosed and/or gave criminals unauthorized access to Mr. Williams' AT&T wireless account, his personal information, and his CPNI by transferring control over Mr. Williams' AT&T wireless number from Mr. Williams' phone to a phone controlled by the third-party hackers.

27. By November 2018, AT&T knew, or should have known, that unauthorized SIM swaps were serious threats to its customers.

28. AT&T was and is fully aware that its customers use two-factor authentication, including two-factor authentication involving phone calls and text messages as "an extra security layer" for their online accounts. AT&T in fact encouraged and still encourages the use of two-factor authentication.

29. AT&T was, including in 2018 and 2019, and is fully aware that criminals use unauthorized SIM swaps as a way to bypass their victims' mobile phone security, including their phone and text based two-factor authentication security.

30. AT&T retains complete control of the protocols, training, procedures, and records for SIM card changes of AT&T customers, even when it contracts out certain of that labor to its authorized retailers or other agents.

31. AT&T's authentication and security protocols, including its "waterfall" authentication protocol, failed to protect Mr. Williams and other AT&T customers from unauthorized SIM swaps. AT&T agents operating in a "retail environment," among other AT&T agents, had the ability to change any AT&T customer's SIM card simply by entering the last four digits of the customer's social security number and noting, without verification or use of the PIN number associated with the relevant account, that they had reviewed the customer's photo identification.

32. This security loophole was used numerous times by AT&T agents to conduct unauthorized SIM swaps to Mr. Williams' account, in the face of specific special instructions from AT&T agents and AT&T's fraud department not to use this loophole to make changes to Mr. Williams' account.

33. AT&T sent Mr. Williams a letter dated May 14, 2019, that states in part that "AT&T's commitment to customer privacy and data security is our top priority and we take this commitment very seriously. We recently determined that an employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization."

34. AT&T sent Mr. Williams a letter dated July 3, 2019, that states in part that "AT&T's commitment to customer privacy and data security is our top priority and we take this commitment very seriously. We recently determined that an

employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization."

35. The details of the six SIM swap attacks on Mr. Williams' account are as follows:

a) November 5, 2018 ("First SIM Swap Attack")

(1) The First SIM Swap Attack, on November 5, 2018, was effectuated by an AT&T agent named Stephen Defiore. Defiore was an employee at Prime Communications, an authorized AT&T retailer. Defiore was an AT&T agent and that AT&T provided with manager-level access to Mr. Williams' account (as well as other customers' accounts). Defiore has since taken responsibility for multiple, unauthorized SIM card changes that occurred at the AT&T store he worked in. AT&T did not fully investigate Stephen Defiore's illegal actions until September 2019, almost a year after he perpetrated the first SIM swap against Mr. Williams (and an unknown number of other AT&T customers).

(2) To effectuate the SIM Swap, Mr. Defiore used, disclosed, and/or permitted access to Mr. Williams' CPNI and personal and account information without authorization.

(3) During the First SIM Swap Attack, after Mr. Defiore used, disclosed, and/or permitted access to Mr. Williams' CPNI and gave hacker(s) access to Mr. Williams' account and his phone via a SIM swap, which included the ability to send and receive phone calls and text messages from Mr. Williams' phone number.

(4) Using the phone number provided to them by AT&T in the First SIM Swap, the hacker(s) accessed Mr. Williams' online accounts, including his Coinbase and

Slush Pool accounts, as well as his Gmail, Twitter, Instagram, DropBox, Google Drive, and LinkedIn accounts.

(5) Upon accessing Mr. Williams' Slush Pool account, the hacker(s) redirected Mr. Williams' bitcoin rewards to their own cryptocurrency wallet, locked the wallet configuration, and denied Mr. Williams access to the interface, which stripped him of his access, operation, or control of his mining operation. The hacker(s) also transferred around .23 bitcoin (at that time worth around $1,500) to their bitcoin wallet.

(6) These actions compromised Mr. Williams' bitcoin mining operation, and all of the cryptocurrency rewards from the mining rigs were funneled to the hacker(s). Mr. Williams had to hire a third party and reconfigure all of his mining rigs. The reconfiguration process took about five days, and during that period, Mr. Williams was unable to mine and lost the ability to earn from those rigs.

(7) The hacker(s) took over Mr. Williams' Gmail account, and accessed, stole, compromised, and took control over a decade's worth of highly sensitive personal information contained in Mr. Williams' Gmail account, including his home address, his social security number, his family members' social security numbers, copies of his passport, copies of family members' passports, TSA precheck information, sensitive financial and personal documents, including patents, pending patents, and various intellectual property concepts and ideas. Mr. Williams, despite numerous efforts, has been unable to regain access to or control over his Gmail account. Since the First SIM Swap, hackers have used Mr. Williams' Gmail account for their own purposes.

(8) The hacker(s) subsequently used this personal information to extort Mr. Williams. Shortly after the SIM Swap attack, an unknown party texted Williams and told

him that if he did not respond to their threats, "all hell will be let loose." Shortly after the SIM Swap attack, an unknown party texted Williams and told him "Answer the phone or your daughter will go missing tonight." The FBI told Mr. Williams that he and his family's personal identification and financial information were put up for sale on the dark web.

(9) Mr. Williams and his family were terrified. Mr. Williams called the FBI and the local police. The local police department said there was nothing they could do to protect Mr. Williams and his family, except add more neighborhood patrols. They asked Mr. Williams if he had a concealed carry license and, when he said he did, they encouraged Mr. Williams to carry a gun with him at all times. Mr. Williams had never regularly carried a gun before the SIM swap attack. However, after he received these texts, he began to arm himself in order to ensure the safety of himself and his family. He also began to stay up all night to watch the outside of his home to ensure no intruders or nefarious individuals came around.

(10) On or about November 6, 2018, after the First SIM Swap Attack, Mr. Williams contacted AT&T and asked what measures AT&T could take to stop this from happening to him again.

(11) AT&T represented to Mr. Williams that it would add extra security to AT&T's record of Mr. Williams' account, specifically by making changes and notations in his account, which specified that his SIM card could only be changed to a new phone (1) via an in-person request in a specific, identified Raleigh AT&T store, and (2) if Mr. Williams presented two passports (current and expired) to the store employees to confirm his identity.

(12) On or about November 6, 2018, Mr. Williams further informed AT&T that he was a financial manager involved with cryptocurrency trading and had digital currency accounts, and that he was at a heightened risk of SIM swap attacks.

(13) At the time of the First SIM Swap Attack, AT&T also knew that improper procedures and systems to safeguard customer data could allow its employees to authorize customers' accounts and data and sell that to third parties, as occurred in the 2015 FCC enforcement action.

(14) In reliance on AT&T's representations that it would add extra security to his account, Mr. Williams decided not to close his AT&T wireless account.

b) December 1, 2018 ("Second SIM Swap Attack")

(1) Notwithstanding the foregoing, on December 1, 2018, AT&T used, disclosed, and/or permitted access to Mr. Williams' CPNI and performed a second unauthorized SIM swap on Mr. Williams' account.

(2) Mr. Williams was in Greensboro, North Carolina, attending a soccer tournament and noticed around 4:00 PM that his AT&T wireless phone had lost service. He immediately suspected another SIM Swap.

(3) The next day, on December 2, 2018, Mr. Williams visited the designated AT&T store in Raleigh with two passports. He disabled his SIM Card and bought a new iPhone for around $700. He purchased the new iPhone because AT&T employees told him it would mitigate the risk of another SIM swap attack.

(4) An AT&T employee assisting Mr. Williams showed him a warning message in his account directing AT&T employees not to change the SIM card associated

with Mr. Williams' account unless he requested the change in-person, at a specific and identified AT&T retail store, with two passports verifying his identity.

(5) When Mr. Williams told the AT&T employee about the multiple attacks, the AT&T employee said the warnings were being deleted from his AT&T account.

(6) The AT&T employee also told him he was on a special list of individuals who were at high risk of being SIM swapped.

(7) At the time of the Second SIM Swap Attack, AT&T also knew or should have known that Mr. Williams was at a heightened risk after (1) he informed AT&T employees that he had digital currency accounts, a risk factor AT&T has acknowledged, and (2) he had previously been the target of a SIM swap attack.

(8) At the time of the Second SIM Swap Attack, AT&T also knew that its account authentication and security procedures and systems were insufficient to safeguard its customer data, and, for example, allowed its employees and agents to access, use, and/or disclose its customers' CPNI and personal and account information without authorization to third parties, similar to AT&T's security failings that resulted in the 2015 FCC enforcement action.

c) December 1, 2018 ("Third SIM Swap Attack")

(1) On the evening of the day he had been at the AT&T store addressing the Second SIM Swap Attack and taking the steps AT&T told him would prevent further SIM-swap attacks, over and above the security measures that AT&T assured him were in place, AT&T used, disclosed, and/or permitted access to Mr. Williams' CPNI and Mr. Williams was SIM swapped for a third time.

(2) Like the other attacks, the hacker(s) attempted to gain access to his online accounts.

(3) When Mr. Williams contacted AT&T to address the Third SIM Swap Attack and to regain control over his AT&T account, the AT&T representative informed Mr. Williams that the warnings regarding not making changes to his SIM card had been deleted from his account. The representative did not tell Mr. Williams why this information had been deleted, or who had deleted it.

(4) A few days later, on or about December 5, 2018, Mr. Williams went to the designated AT&T store in Raleigh to discuss the Third SIM Swap Attack. The employees at the store confirmed that there was a note in his account stating that AT&T should not effectuate a SIM card change unless Mr. Williams asked in person at the designated AT&T store and presented two valid passports. Specifically, the account notes associated with Mr. Williams' AT&T mobile phone number contained:

i. A November 6, 2018, entry entitled "Special Instructions" that states: "Customer was previous victim of Account Takeover on 11/05/18. Please use caution when making account changes/placing order."

ii. A December 3, 2018, entry entitled "Special Instructions" that states: "Customer has verified himself with ID and passcode with manager. Customer has given instructions that transactions can only be made in person with ID and passcode verification… Do not verify by last 4 of ssn….12/03/18 **FRAUD DEPT DO NOT REMOVE** Customer was previous victim of Account Takeover on xx/xx/xx. Please use caution when making account changes/placing order."

iii. A December 5, 2018, entry entitled "Special Instructions" that states: "*FRAUD DEPT DO NOT REMOVE** Account holder lives in NC state and scammers went to OK state att cor store with ID to update sim card multiple times! AH is requesting to verify both the NC state issued driver license and passport before changing sim cards or make changes to the account!"

(5) Importantly, the Account Notes do not contain any note from before December 3, 2018, that is consistent with AT&T's representation in November 2018 that Mr. Williams' identity would have to be confirmed with two passports before AT&T would approve a SIM card change on his account.

(6) Upon seeing the threats Mr. Williams had been receiving after the SIM swap attacks, an AT&T employee at the store called the local police. When the police officers arrived, Mr. Williams told them about the situation, including the threats against himself and his family, and the police again encouraged him to carry a gun.

(7) At the time of the Third SIM Swap Attack, AT&T also knew or should have known that Mr. Williams was at a heightened risk after (1) he informed AT&T employees that he had digital currency accounts, a risk factor AT&T has acknowledged, and (2) he had previously been the target of a SIM swap attack.

(8) At the time of the Third SIM Swap Attack, AT&T also knew that its account authentication and security procedures and systems were insufficient to safeguard its customer data, and, for example, allowed its employees and agents to access, use, and/or disclose its customers' CPNI and personal and account information without authorization to third parties, similar to AT&T's security failings that resulted in the 2015 FCC enforcement action.

d) February 4, 2019 ("Fourth SIM Swap Attack")

(1) On February 4, 2019, AT&T employees again used, disclosed, and/or permitted access to Mr. Williams' CPNI and permitted hacker(s) to perform an unauthorized SIM-swap on Mr. Williams' account, and in doing so, deliberately ignored all the security measures it claimed it had put into place to protect Mr. Williams' account.

(2) At approximately 9:30 PM on February 4, 2019, Mr. Williams noticed his SIM card was deactivated. He contacted AT&T and asked them to immediately disable his phone so the hacker(s) would not have service.

(3) Before the phone was disabled, and while the hacker(s) had control over Mr. Williams' AT&T wireless number, they used that control to access Mr. Williams' accounts on various cryptocurrency exchange platforms, including his Coinbase and Gemini accounts.

(4) The hacker(s) also accessed Mr. Williams' Twitter account again and solicited the exchange of currency from his friends and associates.

(5) In order to address this latest SIM swap attack, Mr. Williams had to buy a plane ticket back to North Carolina from where he was staying in Islamorada, Florida.

(6) At the designated Raleigh AT&T store, an AT&T employees informed Mr. Williams that his SIM card had been swapped the night before via email after an online AT&T representative changed Mr. Williams' four-digit pin password for the benefit of the hacker(s). After each SIM swap attack, Mr. Williams changed his four-digit pin password, yet he continued to be hacked.

(7) At the time of the Fourth SIM Swap Attack, AT&T also knew or should have known that Mr. Williams was at a heightened risk after (1) he informed AT&T

employees that he had digital currency accounts, a risk factor AT&T has acknowledged, and (2) he had previously been the target of SIM swap attacks.

(8) At the time of the Fourth SIM Swap Attack, AT&T also knew that its account authentication and security procedures and systems were insufficient to safeguard its customer data, and, for example, allowed its employees and agents to access, use, and/or disclose its customers' CPNI and personal and account information without authorization to third parties, similar to AT&T's security failings that resulted in the 2015 FCC enforcement action.

e) February 6, 2019 ("Fifth SIM Swap Attack")

(1) Less than 24 hours after his visit to the Raleigh AT&T store, on February 6, 2019, at around 1:30 AM, AT&T used, disclosed, and/or permitted access to Mr. Williams' CPNI and he was subjected to the Fifth SIM Swap Attack.

(2) Mr. Williams noticed that he suddenly lost AT&T service and was only able to connect to WiFi. He attempted to contact AT&T, but he had to wait until AT&T's Fraud Department opened at 8 AM the next morning.

(3) During this attack, the hacker(s) deleted Mr. Williams' Slush Pool account, essentially making his mining rigs useless. The hacker(s) also froze his Gemini account and attempted to steal 51 BTC.

(4) At the designated Raleigh AT&T store, an AT&T employee spoke with the AT&T Fraud Department, who informed her that Mr. Williams' four-digit PIN password had been changed online, and then his SIM card was changed over the phone by an AT&T employee named Rex Mostoles.

(5) At that time, there had been a note in Mr. Williams' AT&T account in large, red font that stated AT&T employees were not to make any account changes, including SIM swaps, via phone call or email. Specifically, the account contained a February 4, 2019, entry entitled "Special Instructions" that stated: "TO ACCESS THE ACCOUNT MUST IDENTIFY ACCOUNT HOLDER VIA 2 PASSPORTS AND I.D. Do not make any changes over the phone at the request Jason Williams verified in store with 2 passports and 1 drivers license." This notation would have appeared prominently in the system that AT&T employees use to view a customer's account notes.

(6) At the time of the Fifth SIM Swap Attack, AT&T also knew or should have known that Mr. Williams was at a heightened risk after (1) he informed AT&T employees that he had digital currency accounts, a risk factor AT&T has acknowledged, and (2) he had previously been the target of a SIM swap attack.

(7) At the time of the Fifth SIM Swap Attack, AT&T also knew that its account authentication and security procedures and systems were insufficient to safeguard its customer data, and, for example, allowed its employees and agents to access, use, and/or disclose its customers' CPNI and personal and account information without authorization to third parties, similar to AT&T's security failings that resulted in the 2015 FCC enforcement action.

(8) Mr. Williams lost his $1.4 million investment in these servers. He also lost the ability to mine bitcoin, which at that time he had been mining around 5-9 BTC per month.

f) February 8, 2019 ("Sixth SIM Swap Attack")

(1) On February 8, 2019, Mr. Williams suffered the Sixth SIM Swap Attack, when AT&T again used, disclosed, and/or permitted access to his CPNI and effectuated a fraudulent transfer of his SIM card.

(2) Following this SIM swap attack, the hacker(s) transferred $6,500 from Mr. Williams' bank account to his Coinbase account and purchased cryptocurrency, and subsequently blocked Mr. Williams' access to his Coinbase account.

(3) Mr. Williams was informed that the Sith SIM Swap Attack had been effectuated by an AT&T employee named Vennessa. AT&T effectuated this SIM swap notwithstanding that none of the security measures, which AT&T had assured Mr. Williams were in place, had been complied with.

(4) Mr. Williams decided to change providers following this Sixth SIM Swap Attack. Associates at the AT&T store told him that because he had only recently purchased his iPhone (following the Second SIM Swap Attack in December 2018), he was not eligible to "unlock" it, and thus if he wanted to change providers, he would need to buy a new iPhone and port his phone number to that provider.

(5) Mr. Williams proceeded to purchase a new iPhone and have his phone number ported over to his new account at Verizon.

(6) At the time of the Sixth SIM Swap Attack, AT&T also knew or should have known that Mr. Williams was at a heightened risk after (1) he informed AT&T employees that he had digital currency accounts, a risk factor AT&T has acknowledged, and (2) he had previously been the target of a SIM swap attack.

(7) At the time of the Sixth SIM Swap Attack, AT&T also knew that its account authentication and security procedures and systems were insufficient to safeguard its customer data, and, for example, allowed its employees and agents to access, use, and/or disclose its customers' CPNI and personal and account information without authorization to third parties, similar to AT&T's security failings that resulted in the 2015 FCC enforcement action.

36. AT&T failed to implement security practices and protocols that would have prevented the blatant and repeated unauthorized SIM swaps of Mr. Williams' mobile account.

37. AT&T failed to train, educate, and/or supervise its employees and agents tasked with authorizing and effectuating customer SIM card changes to, among other things, implement and adhere to AT&T existing account authorization and security practices and protocols, and, as such, failed to prevent its employees and agents from repeatedly ignoring those practices and protocols and from repeatedly making unauthorized SIM card changes to his account.

38. AT&T employees ignored and even deleted instructions that AT&T informed Mr. Williams that it had placed on his wireless account in order to prevent additional SIM swaps. AT&T also accessed his account without permission and changed his security passcode.

39. Each of the SIM swaps on Mr. Williams' account were intentionally executed by AT&T agents, who either were criminals or intentionally, knowingly, recklessly, and/or negligently conducted the SIM swaps on behalf of criminals,

and absent the conduct of AT&T's employees, the criminals would not have been able to access Mr. Williams' accounts.

40. AT&T did not timely notify Mr. Williams that his CPNI had been accessed without his authorization. It was not until months after the Sixth SIM Swap, in a letter dated May 14, 2019, that AT&T wrote him a letter stating: "We recently determined that an employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization." Mr. Williams received another letter from AT&T to this same effect, that was dated July 3, 2019.

41. The six SIM swap attacks on Mr. Williams caused him damages, including:

a) Pecuniary monetary damages from:

(1) Assets stolen from online accounts, including .23 bitcoin stolen during the First SIM Swap Attack (had a then-present value of around $1,500).

(2) Cost of airplane ticket from Florida to North Carolina, which Mr. Williams needed to purchase during the Fourth SIM Swap Attack in order to return to North Carolina to address the attack at the designated AT&T retail store in Raleigh.

(3) Cost of purchasing two new iPhones, about $700 each. The first new iPhone was purchased during the Second SIM Swap Attack, at the recommendation of AT&T employees who told Mr. Williams it would mitigate the risk of another SIM swap attack. The second new iPhone was purchased following the Sixth SIM Swap attack, because upon deciding to change providers, AT&T associates told Mr. Williams that because his current iPhone had been bought just a few months before (during the Second

SIM Swap Attack), he was not eligible to "unlock" it, and thus would need to go to his new carrier, buy another new iPhone, and port his phone number to his new iPhone.

(4) Costs Mr. Williams incurred in investigating who accessed his mobile device and damaged information on it.

(5) Destruction of Mr. Williams' profitable cryptocurrency mining operation, which he had invested over $2 million in, detailed herein.

iv. Mr. Williams was and is the sole member of Apollo, a limited liability company, through which he operated a successful Bitcoin mining operation.

v. Cryptocurrency mining is a process by which new cryptocurrency is introduced into the existing circulating supply, as well as a way to secure the network on which the cryptocurrency operates.

vi. Cryptocurrency mining is extremely technologically complex and requires a complicated technical set up as well as large amounts of electrical power.

vii. From February 2018 until May 14, 2019, Mr. Williams invested over $2 million in his cryptocurrency mining operation, $1.4 million on which was spent on servers powerful enough to compute the cryptographic hash required to successfully mine.

viii. By November 2018, Mr. Williams was successfully mining between seven and twelve bitcoins per month. Each bitcoin was worth approximately $6,381 at the beginning of November 2018, putting Mr. Williams' accumulated bitcoin holdings at approximately $450,000 as of that date. Mr. Williams' mines were linked to, and these rewards were sent to (and accumulated in) an account Mr. Williams set up with an online mine pooling app called Slush Pool.

ix. Mr. Williams was entitled to all of the proceeds from Apollo and its Bitcoin mining operation.

x. All of the proceeds from Mr. Williams' Bitcoin mining operation were deposited directly into online cryptocurrency accounts, each of which was accessed via Mr. Williams' personal email, and subject to his sole control. Mr. Williams also received cryptocurrency from other sources in these accounts.

xi. As a result of the First SIM Swap Attack, the hacker(s) were able to divert Mr. Williams' Apollo Bitcoin mining operation proceeds from Mr. Williams' cryptocurrency accounts to an account (or accounts) controlled by the hacker(s).

xii. After the repeated SIM swaps of Mr. Williams' account compromised the safety of this mining operation, Mr. Williams was forced to discontinue it, or risk attacks against his other (as yet un-hacked) operations. Thus, his cryptocurrency mining operation was destroyed.

b) Emotional distress damages resulting from:

(1) Receipt of threatening calls and text messages from unknown individuals threatening his and his family's safety.

xiii. In November 2018, an unknown party texted Mr. Williams and told him that if he did not respond to their threats, they would sell his information on the dark web on a hacker exchange website.

xiv. On November 28, 2018, at approximately 3:40 PM, Mr. Williams began receiving threatening text messages from an unfamiliar phone number with a California area code. The texts contained Mr. Williams' name, home address, and social security number. The text threatened Mr. Williams' wife and

daughter and attempted to extort him for money. Mr. Williams received another text later the same evening from the same number, again threatening that one of his daughters would be kidnapped if he did not pay a ransom in cryptocurrency. ("Answer the phone or your daughter will go missing tonight.")

xv. On December 1, 2018, at approximately 9:55 PM, Mr. Williams received a text from an unfamiliar phone number that said "Hello Jason Williams." At 2:53 AM the next morning and at 2:25 PM the next day, he received two more text messages: "Hello?" and "You have until today to respond or all hell will be let loose."

(2) Local police telling Mr. Williams that they could not protect him or his family and advising him to be "ready to use" a gun to protect himself and his family.

(3) Purchasing a gun, silencer, and other firearm accessories, at the police's advice and in response to the threats that followed the SIM swaps. Taking home invasion and defense training.

(4) FBI agents telling Mr. Williams that his and his family's personal information had been released onto the "Dark Web," where it was available to criminals and hackers.

(5) Experiencing harm to his reputation after criminals used Mr. Williams' phone number to impersonate him and convince an acquaintance and business associate to transfer Bitcoin to them.

(6) Hackers compromising Mr. Williams' online accounts, including his personal Gmail account, and the information within those accounts.

(7) Never being able to recover access to several personal accounts, including his Gmail account, which has been stolen by and used by criminals and which contains up to a decade's worth of emails and other personal and financial information.

(8) Uncovering information from Google and one of Mr. Williams' cryptocurrency accounts demonstrating that hackers have continued to use his email and cryptocurrency account to send misleading emails and conduct unauthorized and likely unlawful financial transactions.

(9) Permanently losing peace of mind with regard to receiving telephone calls. Because Mr. Williams' phone number has been widely disseminated by the hackers, Mr. Williams no longer answers any calls on his cell phone unless the number is in his contacts and does not have voicemail capabilities.

(10) Undertaking the difficult task of explaining to his children the theft, the threat of kidnapping, and the threat posed by criminals who have stolen and have access to Mr. Williams and his family's personal, personal identification, and financial information, who now express fears of hackers and robbers and feelings of instability.

(11) Hackers sending threatening messages to family group chats.

(12) Police having to come to the Williams' home.

(13) Mr. Williams' daughter continuing to suffer from night terrors that some unknown, shadowy man is attempting to kidnap her.

(14) Experiencing many nights when he was unable to sleep during the period that Mr. Williams was subject to AT&T's SIM swaps, between November 2018 and February 2019 and thereafter, because Mr. Williams was so afraid for his and his family's safety. During those nights, Mr. Williams would stay awake with a gun in hand because

he was afraid intruders would come to his home and attempt to harm him or his family. Mr. Williams has also suffered from anxiety and depression because of the SIM swaps.

(15) Continuing fear of what criminals and hackers might do with the personal and financial information that AT&T gave them access to, and how they could use that information to compromise the safety, security, and privacy of Mr. Williams and his family. As just one example, Mr. Williams continues to fear that those criminals who accessed and used his personal email account, and a decade's worth of his personal emails, will use that information to harm or extort him and his family.

42. Before November 5, 2018, the day AT&T first SIM swapped Mr. Williams' phone, he never received text messages and phone calls threatening him and his family.

43. Before November 5, 2018, to Mr. Williams' knowledge, no one ever impersonated him online or over the phone.

44. Before November 5, 2018, to Mr. Williams' knowledge, his online accounts, including his bank accounts and his personal email containing over a decades' worth of his personal and financial information, had never been hacked and compromised.

45. Before November 5, 2018, Mr. Williams had no reason to believe that any of his personal or financial information was available to criminals on the "Dark Web."

46. Since switching from AT&T to Verizon, Williams has not been subject to any additional SIM swaps.

c) Attorneys' fees and costs

d) Pre- and post-judgement interest

e) Treble damages for violations of N.C. Unfair and Deceptive Trade Practices Act, N.C. Gen Sta. Ann. § 75-1.1

B. Plaintiff's Legal Issues

1. General

a) Mr. Williams, in his personal capacity, and as the sole member of Apollo, is entitled to recover all the damages that he suffered personally, and all the damages he suffered as a result of any losses suffered by Apollo, by reason of AT&T's conduct, because (as found by the Court in denying in part AT&T's motion for summary judgment) AT&T owed Mr. Williams a special duty with respect to Apollo.

b) Mr. Williams, in his personal capacity, and as the sole member of Apollo, is entitled to recover all the damages that he suffered personally, and all the damages suffered by Apollo, by reason of AT&T's conduct, because Mr. Williams suffered special damages with respect to Apollo's losses.

c) None of Mr. Williams' existing claims are barred or limited by North Carolina's Economic Loss Doctrine.

d) Punitive Damages: The Court granted AT&T's motion for summary judgment in part, by ruling that Plaintiff is not entitled to recover punitive damages from AT&T. To avoid any later argument of abandonment or waiver on appeal, Mr. Williams contends that: (a) the evidence he will present of AT&T's misconduct would satisfy the

standard for obtaining punitive damages under North Carolina law; (b) AT&T's Wireless Customer Agreement (the "WCA") does not prohibit or prevent Mr. Williams from recovering punitive damages in these circumstances, but if and to the extent that this agreement could be read to do so, that portion of the WCA would be void under North Carolina law limiting and disfavoring exculpation clauses.

2. Violations of the Federal Communications Act ("FCA"), 47 USC § 222, entitled "Privacy of Customer Information."

a) As a common carrier, AT&T is governed by the Federal Communications Act of 1934, as amended ("FCA"), and by corresponding regulations passed by the FCC.

b) Under 47 U.S.C. § 422, AT&T was obligated to protect the confidentiality of Mr. Williams' CPNI and use it only for certain limited purposes.

c) The FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."

d) Under the FCA, AT&T may only use, disclose, or permit access to Mr. Williams' CPNI: (a) as required by law; (b) with his approval; or (c) in its provision of the telecommunications service from which such information is derived or services necessary to or used in the provision of such telecommunications services. Beyond such uses, the Commission's

rules require carriers to obtain a customer's knowing consent before using or disclosing CPNI.

e) Pursuant to the FCA, the FCC has developed rules concerning carriers' obligations to protect customers' CPNI.

f) Pursuant to FCC rules, carriers must: (a) implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI; (b) design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established; and (c) maintain records that track access to customer CPNI records, and show when CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI.

g) Carriers are also required to train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

h) The FCC requires carriers to take reasonable steps to protect their customers' CPNI.

i) The FCC requires carriers to inform customers and law enforcement whenever a security breach results in that customer's CPNI being disclosed to a third party without that customer's authorization.

j) Under the FCA, carriers are liable for their own violations of the FCA, for the acts, omissions, and/or failures of their officers, agents, employees, or other agents, and for any violations that they cause or permit.

k) AT&T used, disclosed, and/or permitted access to Mr. Williams' CPNI without the notice, consent, and/or legal authorization required under the FCA, when its agents and employees accessed Mr. Williams' account without his authorization, and swapped his SIM card.

l) AT&T caused and/or permitted unauthorized third parties to use, disclose, and/or access Mr. Williams' CPNI without Mr. Williams' notice, consent, and/or legal authorization as required under the FCA, by effecting unauthorized SIM-swaps, thus further violating 47 U.S.C. § 222.

m) Mr. Williams has suffered injury to his person, property, health, and/or reputation as a consequence of AT&T's violations of the FCA.

n) AT&T's wrongful conduct was the proximate cause of Mr. Williams' injury.

o) Mr. Williams is entitled to recover all of his damages, together with reasonable attorneys' fees to be fixed by the Court, and collected as part of the costs of this case.

3. Violation of N.C. Unfair and Deceptive Trade Practices Act, N.C. Gen Sta. Ann. § 75-1.1

a) North Carolina's Unfair and Deceptive Trade Practices Act ("NCUDTPA") prohibits any "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."

b) AT&T committed unfair and deceptive trade practices under N.C. Gen. Sta. Ann. § 75-1.1 when AT&T made material misrepresentations

and omissions to Mr. Williams concerning its sale of, and ability to safeguard, Mr. Williams' CPNI, and its ability to prevent unauthorized access thereto.

c) AT&T committed unfair and deceptive trade practices under N.C. Gen. Sta. Ann. § 75-1.1 when AT&T breached its duty to disclose the full and true nature of its inadequate security and data protection practices, and particularly the significant risk that its own employees would reveal and/or sell private customer information and CPNI, which information was known exclusively to AT&T, including while simultaneously advertising its ability to, among other things, protect the security of its customers' accounts and private information, and to anticipate and thwart cyber security threats.

d) A reasonable person would be deceived and misled by AT&T's misrepresentations regarding its safeguarding of customers' personal and proprietary information.

e) A reasonable person would be deceived and misled by AT&T's misrepresentations about the procedures it promised to put in place to protect Mr. Williams' account from being changed unless specific security measures were satisfied, and a reasonable person would have been deceived and misled into believing that AT&T would follow the procedures AT&T promised to put into place, and therefore his account would be safe from future breaches.

f) AT&T committed unfair and deceptive trade practices under N.C. Gen. Sta. Ann. § 75-1.1 when it intentionally misled its customers regarding its data protection practices in order to attract customers and evade prosecution for its unlawful acts.

g) AT&T's actions were in or affecting commerce.

h) AT&T's unfair and deceptive acts were immoral, substantially injurious, deceptive, unethical, and/or oppressive.

i) AT&T's wrongful conduct was the proximate cause of Mr. Williams' injury.

j) Mr. Williams is entitled to recover treble damages pursuant to N.C. Gen. Stat. § 75-16 and attorneys' fees pursuant to N.C. Gen. Stat. § 75-16.1.

4. Negligence / Negligent Infliction of Emotional Distress

a) AT&T owed a duty to Mr. Williams to exercise reasonable care in safeguarding his sensitive personal information – including by designing, maintaining, monitoring, and testing its and its agents', partners', and independent contractors' systems, protocols, and practices.

b) AT&T owed a duty to Williams to protect his sensitive account data from unauthorized use, access, or disclosure – including by ensuring that his CPNI was only used, accessed, or disclosed with proper consent.

c) AT&T owed a duty to Mr. Williams to disclose the material facts concerning its inadequate security practices.

d) AT&T had a special relationship with Williams due to its status as his telecommunications carrier, which provided an independent duty of care.

e) AT&T breached its duties to Mr. Williams, and acted negligently, by:

(1) Failing to implement and maintain adequate security practices to safeguard Mr. Williams' AT&T account information and data – including his CPNI – from unauthorized access, use, and disclosure;

(2) Failing to detect unauthorized access, use, or disclosure of this information and data in a timely manner, including but not limited to unauthorized access by its own agents and employees;

(3) Failing to disclose that AT&T's data security practices were inadequate to safeguard Mr. Williams' information and data;

(4) Failing to supervise its employees and prevent employees from accessing Williams' AT&T account information and data without authorization;

(5) Failing to provide adequate and timely notice of such unauthorized access; and/or

(6) Failing to follow the very security measures which AT&T put into place, and which AT&T promised Mr. Williams had been put into place, as measures to protect Mr. Williams's account from unauthorized third-party SIM-swap attacks.

f) AT&T's breach(es) of its duties was the proximate cause of Mr. Williams' injury.

g) Mr. Williams was a foreseeable victim of AT&T's negligent conduct set forth above.

h) AT&T knew or should have known that unauthorized accesses of Mr. Williams' account by unauthorized third-parties would cause damage to Mr. Williams.

i) Mr. Williams suffered damages as a result of AT&T's breach(es) of its duties and resulting failure to prevent unauthorized accesses to Williams' AT&T account data.

j) AT&T's conduct was negligent.

k) AT&T's conduct went beyond negligence, and was willful, wanton, and grossly negligent.

l) Mr. Williams is entitled to recover damages for all monetary losses he and/or Apollo suffered by reason of AT&T's negligence.

m) Mr. Williams is also entitled to recover damages for his emotional suffering, based on his own suffering and the upheaval in his own life, caused by AT&T's conduct, and based on the emotional damage suffered by his spouse and children, which Mr. Williams witnessed.

n) AT&T's Wireless Customer Agreement does not prohibit or prevent Mr. Williams from recovering damages for emotional suffering in these circumstances, but if and to the extent that the WCA could be read to do so, that portion of the WCA would be void under North Carolina law limiting and disfavoring exculpation clauses.

5. Negligent Supervision

a) AT&T is liable for its agents' and employees' wrongful conduct because AT&T was negligent or reckless in employing and supervising employees in work in involving the risk of harm to others, including to Mr. Williams.

b) AT&T knew or had reason to know that its employees were unfit and were likely to harm others.

c) AT&T was negligent in supervising its employees an in entrusting them with highly sensitive data.

d) AT&T negligently employed certain employees and failed to exercise due care in selecting them.

e) AT&T negligently created the risk that its employees would commit criminal acts against its customers, including Mr. Williams.

f) AT&T was on notice that its employees were behaving negligently, by conducting unauthorized SIM-swaps, but failed to take adequate and timely action to prevent that conduct.

g) The unauthorized SIM-swaps of Mr. Williams' account are directly tied to AT&T's negligence in this regard. Had AT&T built proper systems to effectively authentical and verify consumer consent to SIM-swaps, and to prevent employees from making unauthorized changes customers' SIM cards, or customers' security information, Mr. Williams would not have been injured.

h) Mr. Williams' injury was foreseeable. AT&T was aware that its customer accounts were vulnerable to unauthorized access and sale by

their own employees. AT&T's conduct was the proximate cause of Mr. Williams' injuries.

i) AT&T's conduct was negligent.

j) AT&T's conduct went beyond negligence, and was willful, wanton, and grossly negligent.

k) Mr. Williams is entitled to recover damages for all monetary losses he and/or Apollo suffered by reason of AT&T's negligence.

l) Mr. Williams is also entitled to recover damages for his emotional suffering, based on his own suffering and the upheaval in his own life, caused by AT&T's conduct, and based on the emotional damage suffered by his spouse and children, which Mr. Williams witnessed.

m) AT&T's Wireless Customer Agreement does not prohibit or prevent Mr. Williams from recovering damages for emotional suffering in these circumstances, but if and to the extent that the WCA could be read to do so, that portion of the WCA would be void under North Carolina law limiting and disfavoring exculpation clauses.

6. N.C. Computer Anti-Hacking Statute N.C.G.S.A. § 1-539.2A

a) North Carolina's Anti-Hacking statute prohibits "any person to use a computer or computer network without authority and with intent to. . . [t]emporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network; [c]ause physical injury to the property of another; or [m]ake or cause to be made an unauthorized copy, in any form, including,

but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

b) Per this statute, "a person is 'without authority' when … the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission . . . ."

c) AT&T, through its employees, used a computer or computer network without the right or permission of Mr. Williams, with intent to:

(1) disable and halt data from Mr. Williams' mobile device, and/or

(2) make or cause to be made copies of Mr. Williams' confidential data by conducting a SIM swap and allowing and/or assisting third-party hackers to access and use his confidential data.

d) As a direct and proximate result of AT&T's actions, Williams has sustained monetary losses and costs, in the form of lost revenues and profits and costs to restore data that was improperly altered and/or deleted.

C. Defendant's Factual and Legal Contentions

1. All facts not stipulated to above are in contention and AT&T puts Plaintiff to his proof on each and every fact upon which he bears the burden of proof.

2. AT&T intends to establish that Mr. Williams did not suffer severe emotional distress, and therefore he is not entitled to recover any such damages in this action.

3. AT&T intends to establish that Mr. Williams did not maintain adequate security on his online, financial, cryptocurrency and other accounts at issue in this case and therefore is contributorily negligent to the extent he proves any damages.

4. AT&T intends to establish that Mr. Williams' contract with AT&T for wireless services limits AT&T's liability for his alleged damages.

5. AT&T intends to establish that Mr. Williams damages, if any, were the result of a targeted criminal attack by unknown person or persons for which AT&T has no legal liability.

6. AT&T intends to establish that it did not make any unfair or deceptive misrepresentations or omission and did not engage in any unfair or deceptive acts as alleged by Plaintiff.

7. AT&T intends to establish that it took reasonable steps safeguard Mr. Williams' CPNI, to protect against SIM swap fraud.

8. AT&T intends to establish that Mr. Williams' CPNI was not unlawfully used, disclosed or accessed.

9. AT&T intends to establish that Mr. Williams was not damaged by any use, disclosure or access of his CPNI.

10. AT&T intends to establish that Mr. Williams was reimbursed by his bank for certain amounts he is claiming as damages in this action and therefore is not entitled to recover such damages from AT&T in this action.

11. AT&T intends to establish that Jason Williams' alleged crypto-mining was conducted by Apollo Kids Mining LLC and therefore Jason Williams is not entitled to recover for such alleged damages in this action.

12. AT&T intends to establish that Apollo Kids Mining LLC was not AT&T's customer and therefore neither Apollo Kids Mining LLC or Jason Williams may recover such damages.

13. AT&T intends to establish that Jason Williams' alleged crypto-mining was not profitable and therefore Williams (either individually or through Apollo Kids Mining) is not entitled to recover any such damages.

14. AT&T intends to establish prove that there are no facts which establish that AT&T was negligent in its supervision, training or retention of any AT&T employee, officer, director or managing agent.

15. AT&T intends to establish that it did not violate 47 U.S.C. §222 as to Plaintiff Jason Williams.

16. AT&T intends to establish it did not violate N.C. General Statute §75-1 (North Carolina Unfair and Deceptive Trade Practices Act) as to Plaintiff Jason Williams.

17. AT&T intends to establish that it was not negligent as to Plaintiff Jason Williams.

18. AT&T intends to establish that it was not negligent in its supervision, training or retention of any AT&T employee, managing agent, officer or director.

19. AT&T intends to establish that it did not violate North Carolina's Computer Trespass Law (N.C. General Statute §14-458).

20. AT&T intends to establish Plaintiff Jason Williams is not entitled to recover any attorneys' fees or costs.

21. AT&T intends to establish that Jason Williams is not entitled to pre-judgment interest.

22. AT&T intends to establish that Jason Williams is not entitled to any other category of damages he seeks in his Corrected Complaint.

23. The Court's Order on AT&T's summary judgment motion dismissed Plaintiff's claims for punitive or exemplary damages and therefore these damages should not be at issue in this trial.

24. The Court's Order on AT&T's summary judgment motion dismissed Plaintiff's Count VI for violation of the Computer Fraud and Abuse Act, 18 U.S.C. §1030 and therefore this claim should not be at issue in this trial.

III. EXHIBITS

A. Plaintiff's Exhibits

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-1	Jason Williams' ("Plaintiff") Complaint against AT&T Mobility, LLC ("Defendant"), dated October 25, 2019 ("Complaint")	Doc. No. 02	FRE 402; FRE 403 Unverified Complaint, prejudicial effect outweighs probative value; FRE 611 Attorney testimony, prejudicial effect outweighs probative value; FRE 802 Hearsay; FRE 702; FRE 901
PX-2	Defendant AT&T's Privacy Policy	Doc No. 02-1	FRE 402; FRE 403; FRE 802 Hearsay
PX-3	Lori Cranor, FTC Chief Technologist, *Your mobile phone account could be hijacked by an identity thief*, Federal Trade Commission (June 7, 2016)	Complaint, footnote 41	FRE 402, FRE 403, FRE 802, Hearsay; FRE 702; FRE 901 Not disclosed as an expert in this action, prejudicial effect outweighs probative value, Link in fn 41 does not work "Page Not Found" https://www.ftc.gov/newsevents/blogs/techftc/2016/06/your-

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
			mobile-phone-accountcould-be-hijacked-identity-thief
PX-4	Brian Rexroad, *Secure Your Number to Reduce SIM Swap Scams*, AT&T's Cyber Aware (Sept. 2017)	Complaint, footnote 46	FRE 402, 403, 802, 901 (Not disclosed as an expert in this action, prejudicial effect outweighs probative value; link in footnote appears to be to a different article. (https://about.att.com/pages/cyberaware/ni/blog/sim_swap), hearsay, lack of authentication)
PX-5	*AT&T Tech Channel*, YouTube https://www.youtube.com/user/ATTTechChannel	Complaint, footnote 48	FRE 402, 403, 802, 901 (lack of authentication for Youtube video, actual videos not provided in discovery; prejudicial effect outweighs probative value)
PX-6	*AT&T – Protect Your Network with the Power of &*, VIMEO https://vimeo.com/172399153	Complaint, footnote 49	FRE 402, 403, 802, 901 (lack of authentication for Youtube video, actual videos not provided in discovery; prejudicial effect outweighs probative value)
PX-7	*AT&T Mobile Security*, YouTube (Feb. 12, 2019) https://www.youtube.com/watch?v=KSPHS89VnX0	Complaint, footnote 50	FRE 402, 403, 802, 901 (lack of authentication for Youtube video, actual videos not provided in discovery; prejudicial effect outweighs probative value) Cannot access – "Video Unavailable – video is private"
PX-8	*AT&T Mobile Movement Campaign – Ads*, VIMEO https://vimeo.com/224936108	Complaint, footnote 51	FRE 402, 403, 802, 901 (lack of authentication for Youtube video, actual videos not provided in discovery; prejudicial effect outweighs probative value)
PX-9	AT&T Tech Channel, *The Huntin' and Phishin' Episode*, YouTube https://www.youtube.com/watch?v=3g9cPCiFosk	Complaint, footnote 52	FRE 402, 403, 802, 901 (lack of authentication for Youtube video, actual videos not provided in discovery; prejudicial effect outweighs probative value)
PX-10	AT&T ThreatTraq, *The Real Threat of Insider*	Complaint, footnote 55	FRE 402, 403, 802, 901 (lack of authentication for Youtube video, actual videos not provided in discovery; prejudicial effect

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
	Threats, YouTube (May 5, 2017) https://www.youtube.com/watch?v=ZM5tuNiVsjs		outweighs probative value)
PX-11	AT&T ThreatTraq, *5/31/19 Account-hacking Forum OGusers Hacked*, YouTube (May 31, 2019) https://www.youtube.com/watch?time_continue=234&v=cS4xV3cej3A	Complaint, footnote 60	FRE 402, 403, 802, 901 (prejudicial effect outweighs probative value; lack of authentication for Youtube video, actual videos not provided in discovery; further link does not work, "video unavailable")
PX-12	Defendant AT&T's Memorandum of Law in Support of its Motion to Dismiss Pursuant to Rule 12 (b)(6), 12 (b)(1) and 9(b), dated December 20, 2019	Doc No. 15	FRE 402, 403 (prejudicial effect outweighs probative value); FRE 611 (Attorney arguments/ testimony, prejudicial effect outweighs probative value)
PX-13	Court's March 25, 2020 Order denying Defendant's Motion to Dismiss	Doc No. 20	FRE 402, 403 (Prejudicial effect outweighs probative value)
PX-14	Defendant's Initial Disclosures Pursuant to Fed. R. Civ. Proc. 26 (a)(1), dated May 18, 2020		FRE 401, 402, 403, and 411
PX-15	Plaintiff's Responses and Objections to Defendant's First Set of Interrogatories, dated July 6, 2020		FRE 401, 402, 403, FRE 611
PX-16	Defendant's Answers and Objections to Plaintiff's First Set of Interrogatories, dated July 20, 2020		FRE 401, 402, 403
PX-17	Defendant's Answers and Objections to Plaintiff's First Set of Requests for Production of Documents, dated July 20, 2020		FRE 401, 402, 403
PX-18	Plaintiff's First Supplemental Responses		FRE 401, 402, 403 (Prejudicial effect outweighs probative value)

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
	and Objections to Defendant's First Set of Interrogatories, dated September 28, 2020		FRE 611 (Attorney arguments/ testimony, reference to unverified pleading and supplemental response to interrogatory 11, references to Rule 12(b)(6) order regarding sufficiency of Complaint allegations under the Rule 12 standard)
PX-19	Defendant's First Supplemental Initial Disclosures Pursuant to F.R.C.P. 26(a)(1), dated October 21, 2020		FRE 401, 402, 403, and 411
PX-20	Copy of email chain between Google and Mr. Williams' counsel, Joseph Gallo, dated April 1, 2021	Transmitted to AT&T on April 22, 2021	FRE 802 Hearsay; FRE 901
PX-21	Plaintiff's Second Supplemental Response and Objections to Defendant's First Set of Interrogatories, dated April 20, 2021		FRE 401, 402, FRE 403 (Prejudicial effect outweighs probative value) FRE 611 (Attorney arguments/ testimony, reference to unverified pleading; FRE 802 (Hearsay of unknown declarants in second supplemental response to interrogatory 11)
PX-22	Plaintiff's Expert Report of Jameson Lopp, dated July 14, 2021 (w/ supporting exhibits 1-8)		FRE 602, FRE 701, 702, and FRE 802
PX-23	Defendant's Expert Report of Stephen C. Mott, dated August 2, 2021 (w/ supporting exhibits A-D)		No objection
PX-24	Defendant's Expert Report of Ryan Garlick, dated August 2, 2021 (w/ supporting exhibits A-E)		No objection
PX-25	Defendant's Expert Report of Richard A. Sanders,		No objection

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
	dated August 2, 2021 (w/ supporting exhibits A-E)		
PX-26	Plaintiff's Responses and Objections to Defendant's Second Set of Interrogatories, dated August 13, 2021		FRE 401, 402, 403, 611, 802
PX-27	Defendant's Expert Rebuttal Report of Richard A. Sanders, dated August 18, 2021 (w/ supporting exhibits A-F)		No objection
PX-28	Plaintiff's Expert Rebuttal Report of Jameson Lopp, dated August 20, 2021		FRE 602, 701, 702, and FRE 802
PX-29	Plaintiff's Responses to AT&T's First Requests for Admission, dated September 17, 2021		FRE 401, 402, FRE 403 (Prejudicial effect outweighs probative value) FRE 611 (Attorney arguments/ testimony, reference to unverified pleading; FRE 802
PX-30	Copy of letter from Mr. Williams' counsel, Christopher LaVigne, to AT&T's counsel, Michael Breslin, dated September 24, 2021		FRE 802 - Hearsay; FRE 602 Lack of personal knowledge
PX-31	Plaintiff's First Supplemental Responses and Objections to Defendant's Second Set of Interrogatories, dated November 12, 2021		FRE 401, 402, FRE 403 (Prejudicial effect outweighs probative value) FRE 611 (Attorney arguments/ testimony, reference to unverified pleading; and FRE 802 Hearsay
PX-32	Deposition Transcript of AT&T employee and 30(b)(6) witness Ray Hill, taken on November 17, 2021		Violates FRCP 26 (a)(3) and Pre-trial Order (Dkt 159); Failure to designate specific portions of the transcript to be used. AT&T reserves the right to assert objections to any specific page

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
			and line number offered by Plaintiff
PX-33	Deposition Transcript of AT&T employee and 30(b)(6) witness Valerie Scheder, taken on November 30, 2021		Violates FRCP 26 (a)(3) and Pre-trial Order (Dkt 159); Failure to designate specific portions of the transcript to be used. AT&T reserves the right to assert objections to any specific page and line number offered by Plaintiff
PX-34	Defendant AT&T Mobility, LLC's Amended Privilege Log, dated February 15, 2022		FRE 401, 402, 403, FRE 501-02 – Privilege
PX-35	Deposition Transcript of Plaintiff, Jason Williams, taken on February 23, 2022		Violates FRCP 32. Violates FRCP 26 (a)(3) and Pre-trial Order (Dkt 159); Failure to designate specific portions of the transcript to be used. AT&T reserves the right to assert objections to any specific page and line number offered by Plaintiff
PX-36	Deposition Transcript of AT&T employee and 30(b)(6) witness Robert Arno, taken on February 28, 2022		Violates FRCP 26 (a)(3) and Pre-trial Order (Dkt 159); Failure to designate specific portions of the transcript to be used. AT&T reserves the right to assert objections to any specific page and line number offered by Plaintiff
PX-37	Invoices from Dazzle Manufacturing Ltd.	JW_0001-02	FRE 401, 402, 403, 802, 901
PX-38	Email chain between Jason Williams and First Citizen's bank	JW_0004-09	FRE 802 – Hearsay, FRE 401, 402, 403, FRE 901
PX-39	Google security alert sent to Jason Williams	JW_0010	FRE 802 - Hearsay, FRE 401, 402, 403, FRE 901
PX-40	Gemini security alert sent to Jason Williams	JW_0011	FRE 802 - Hearsay; FRE 401, 402, 403, FRE 901

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-41	Text messages from unknown sender sent to Jason Williams	JW_0012	FRE 802 - Hearsay; FRE 403, Irrelevant, prejudicial effect outweighs probative value
PX-42	Pictures of Jason Williams' mining rigs	JW_0013-14	FRE 401, 402, 403, FRE 901
PX-43	Google security alert sent to Jason Williams	JW_0018	FRE 802 - Hearsay; FRE 901- Lack of authentication
PX-44	Jason Williams' note regarding conversation with "Vennessa"	JW_0028	FRE 403 (Prejudicial effect outweighs probative value; FRE 802 – Hearsay, unidentifiable declarant statement; FRE 901- Lack of authentication
PX-45	Text message from unknown sender sent to Jason Williams	JW_0029	FRE 802 - Hearsay; FRE 403, Irrelevant, prejudicial effect outweighs probative value
PX-46	Email chain between Jason Williams and FBI agents	JW_0032	FRE 401, 402, 403, FRE 802, FRE 901
PX-47	Copy of text messages received by Mr. Williams from unknown sender	JW_0034-35	FRE 802 - Hearsay; FRE 403, Irrelevant, prejudicial effect outweighs probative value
PX-48	Copy of text messages received by Mr. Williams from unknown sender	JW_0036	FRE 802 - Hearsay; FRE 403, Irrelevant, prejudicial effect outweighs probative value
PX-49	Text chain between Mr. Williams and friend	JW_0037-38	FRE 802 - Hearsay; FRE 403, Irrelevant, prejudicial effect outweighs probative value
PX-50	Text chain between Mr. Williams and friend	JW_0039	FRE 802 - Hearsay; FRE 403, Irrelevant, prejudicial effect outweighs probative value
PX-51	Copy of a "2018 Hack Tracker" document	JW_0040-41	FRE 401, 402, 403, FRE 802, FRE 901
PX-52	Google security alert sent to Jason Williams	JW_0043	FRE 802 – Hearsay
PX-53	Email chain between Jason Williams and Gemini	JW_0048-49	FRE 802 – Hearsay
PX-54	Google account recovery form	JW_0051-54	FRE 802 - Hearsay; FRE 901 – Lack of authentication

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-55	Email chain between Jason Williams and Coinbase	JW_0055-57	FRE 802 - Hearsay; FRE 901 – Lack of authentication
PX-56	Email chain between Jason Williams and Gemini	JW_0058-64	FRE 802 - Hearsay; FRE 901 – Lack of authentication
PX-57	Anexio Agreement	JW_0066-70	FRE 401, 402, 403, FRE 802, FRE 901
PX-58	Security settings and account access logs for Mr. Williams' Gemini account	JW_0077-83	FRE 802 – Hearsay
PX-59	Gemini transaction logs for Mr. Williams' account	JW_0084	FRE 802 - Hearsay; FRE 901 – Lack of authentication
PX-60	Security settings for Mr. Williams' Slush Pool account	JW_0085-87	FRE 401, 402, 403, FRE 802, FRE 901
PX-61	Slush Pool BTC payout logs for Mr. Williams' account	JW_0088	FRE 401, 402, 403, FRE 802, FRE 901
PX-62	Slush Pool activity logs for Mr. Williams' account	JW_0089	FRE 401, 402, 403, FRE 802, FRE 901
PX-63	Slush Pool BTC reward logs for Mr. Williams' account	JW_0090	FRE 401, 402, 403, FRE 802, FRE 901
PX-64	Cryptocurrency mining accounting documents	JW_0091-97	FRE 401, 402, 403, FRE 802, FRE 901
PX-65	Gemini Bitcoin deposit email alert	JW_1930	FRE 401, 402, 403, FRE 802, FRE 901
PX-66	Gemini Bitcoin deposit email alert	JW_2018	FRE 401, 402, 403, FRE 802, FRE 901
PX-67	Email chain between Jason Williams and First Citizen's bank	JW_2096-97	FRE 401, 402, 403, FRE 802, FRE 901
PX-68	Email chain between Jason Williams and First Citizen's bank,	JW_2098-99	FRE 401, 402, 403, FRE 802, FRE 901
PX-69	Email security alerts from Coinbase	JW_2100-02	FRE 401, 402, 403, FRE 802, FRE 901
PX-70	Email security alerts from Google	JW_2114-17	FRE 401, 402, 403, FRE 802, FRE 901

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-71	Gemini Bitcoin deposit email alert	JW_2155	FRE 401, 402, 403, FRE 802, FRE 901
PX-72	Email chain between Jason Williams and FBI agent	JW_2170-80	FRE 401, 402, 403, FRE 802, FRE 901
PX-73	Email from Jason Williams to Liz Layman	JW_2200	FRE 401, 402, 403, FRE 802, FRE 901
PX-74	Email chain between Jason Williams and Gemini	JW_2230-33	FRE 401, 402, 403, FRE 802, FRE 901
PX-75	Email chain between Jason Williams and Gemini	JW_2241-42	FRE 401, 402, 403, FRE 802, FRE 901
PX-76	Email chain between Jason Williams and Gemini	JW_2245	FRE 401, 402, 403, FRE 802, FRE 901
PX-77	Email chain between Jason Williams and Anexio	JW_2388-91	FRE 401, 402, 403, FRE 802, FRE 901
PX-78	Email chain between Jason Williams and First Citizen's bank	JW_2417-22	FRE 401, 402, 403, FRE 802, FRE 901
PX-79	Email chain between Jason Williams and Jason Cross	JW_2430	FRE 401, 402, 403, FRE 802, FRE 901
PX-80	Email chain between Jason Williams and Coinbase	JW_2448-50	FRE 401, 402, 403, FRE 802, FRE 901
PX-81	Email chain between Jason Williams and First Citizen's bank	JW_2458-60	FRE 401, 402, 403, FRE 802, FRE 901
PX-82	Email chain between Jason Williams and FBI agents	JW_2461-63	FRE 401, 402, 403, FRE 802, FRE 901
PX-83	Email chain between Jason Williams and Coinbase	JW_2483-88	FRE 401, 402, 403, FRE 802, FRE 901
PX-84	Email security alert from Twitter	JW_2553	FRE 401, 402, 403, FRE 802, FRE 901
PX-85	Copy of Application for Tax Paid Transfer and Registration of Firearm	JW_3293-98	FRE 401, 402, 403, FRE 802, FRE 901
PX-86	"How Criminals Recruit Telecom Employees to Help	JW_3321-26	FRE 802 – Hearsay; FRE 702 – author not designated as expert in this action; FRE 403- confuses

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
	Them Hijack SIM Cards," dated August 3, 2018		issues and prejudicial effect outweighs probative value
PX-87	"AT&T Contractors and a Verizon Employee Charged with Helping SIM Swapping Criminal Ring," dated May 13, 2019	JW_3327-30	FRE 802 – Hearsay; FRE 702 – author not designated as expert in this action; FRE 403- confuses issues and prejudicial effect outweighs probative value
PX-88	AT&T's September 23, 2021 "Cyber Aware" blog post "Better Protect Your Online Accounts with 'Two-Factor Authentication"	JW_3331-33	FRE 402, Relevance; FRE 403, confusing, FRE 802 Hearsay
PX-89	"Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency," dated August 21, 2017	JW_3334-37	FRE 802 – Hearsay; FRE 702 – author not designated as expert in this action; FRE 403- Confuses issues and prejudicial effect outweighs probative value
PX-90	Gemini transaction logs for Mr. Williams' account	JW_3338	FRE 602; FRE 901
PX-91	WhatsApp message between JP Baric and Mr. Williams with attachments	JW_3339-58	FRE 401, 402, 403, FRE 802; FRE 602, FRE 901
PX-92	Documents produced by Alorica Inc.	ALORICA 000001-145	FRE 602; FRE 901
PX-93	Documents produced by Coinbase	Transmitted to AT&T on February 24, 2021 and March 19, 2021	FRE 602; FRE 901
PX-94	Documents produced by Concentrix	CONCENTRIX 000001-1998	FRE 602; FRE 901
PX-95	Documents produced by First Citizens Bank	FirstCitizens_ 0001-15	FRE 602; FRE 901
PX-96	Documents produced by Gemini	GEMINI_ 0001-0089	FRE 602; FRE 901

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-97	Documents produced by Google LLC	Google_ 000001-05	FRE 602; FRE 901
PX-98	Documents produced by Prime Communications	PRIME000001-117	FRE 602; FRE 901
PX-99	Documents produced by TPUSA, Inc.	TPUSA_ 00000001-159	FRE 602; FRE 901
PX-100	Email communications between AT&T and Prime Communications	PRIME000001-04	FRE 802 Hearsay
PX-101	AT&T's ID Verification processes in OPUS	ATT-WIL-00188-194	FRE 401, 402, 403
PX-102	AT&T's informational pages regarding Social Engineering Awareness - Compliance	ATT-WIL-00284-294	FRE 401,402, 403
PX-103	AT&T's Social Engineering Awareness Training	ATT-WIL-00381-466	FRE 401, 402, 403
PX-104	CPNI AT&T University Slides	ATT-WIL-00467-571	FRE 401, 402, 403
PX-105	AT&T's informational pages regarding Social Engineering Awareness for Authorized Retail	ATT-WIL-00572-601	FRE 401, 402, 403
PX-106	AT&T's account notes associated with Mr. Williams' phone number	ATT-WIL-00624-690	FRE 401, 402, FRE 403, FRE 802 Hearsay
PX-107	AT&T's Exclusive National Dealer Agreement with Prime Communications, L.P.	ATT-WIL-01223-1277	FRE 401, 402, 403 - Confuses issues and prejudicial effect outweighs probative value
PX-108	Excerpt of AT&T's Wireless Customer Agreement	ATT-WIL-01536	FRE 106 – Incomplete
PX-109	AT&T's SIM Replacement Policy	ATT-WIL-01692-1706	FRE 401, 402, 403

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-110	AT&T's Retail Account Access Policy	ATT-WIL-01981-2000	FRE 401, 402, 403
PX-111	AT&T's Fraud and Social Engineering Training	ATT-WIL-02101-2102	FRE 401, 402, 403
PX-112	Transcript of podcast interview with Mr. Williams	ATT-WIL-02317-2320	FRE 402, FRE 802 Hearsay
PX-113	AT&T's informational pages regarding SIM Replacement Policy_Postpaid Customer	ATT-WIL-02775-2778	FRE 401, 402, 403
PX-114	AT&T's informational pages regarding Wireless Account Changes – OPUS	ATT-WIL-02825-2826	FRE 401, 402, 403
PX-115	AT&T's SIM Swap Restriction Letter to All Authorized Retailers	ATT-WIL-02953	FRE 407; Hearsay 802
PX-116	AT&T's Weekly Sync: AT&T and Prime Back Office Teams	ATT-WIL-03153-3156	FRE 407, Hearsay 802
PX-117	AT&T's Weekly Sync: AT&T and Prime Back Office Teams	ATT-WIL-03254-3258	FRE 407, Hearsay 802
PX-118	Redacted list of SIM swap victims	ATT-WIL-03260	FRE 401, 402, FRE 403 - Confuses issues and prejudicial effect outweighs probative value; FRE 802 Hearsay; FRE 901
PX-119	Documents regarding SIM Swap Model V2.1, obtained from "wiki.web.att.com"	ATT-WIL-03881-3888	FRE 407 – Subsequent remedial measures
PX-120	AT&T document entitled "Unauthorized SIM Swaps"	ATT-WIL-03915-3917	FRE 407 – Subsequent remedial measures; FRE 902 Authentication
PX-121	AT&T's documents entitled "What We've Done So Far for Hijack Prevention"	ATT-WIL-04856-4863	FRE 407 – Subsequent remedial measures
PX-122	Email from Tony Le to Eric Brandt, et al.	ATT-WIL-04985-4987	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-123	Email from Peter Coulter to Brian Rexroad, et al.	ATT-WIL-05266-5270	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-124	Email from Kristi Parrott to Sherie Britain, Ray Hill	ATT-WIL-05523-5524	FRE 802 – Hearsay
PX-125	Email from Kristi Parrott to Nena Romano, Valerie Scheder	ATT-WIL-05525-5528	FRE 802 – Hearsay
PX-126	Email from Kristi Parrott to Sherie Britain; et al.	ATT-WIL-05565-5568	FRE 802 - Hearsay
PX-127	Email from Tony Le to Peter Brizo; et al.	ATT-WIL-05624-5627	FRE 802 – Hearsay
PX-128	Anomaly & Data Integrity team meeting slides	ATT-WIL-05864-5873	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-129	Email from James Jones to Cheri Kerstetter; et al.	ATT-WIL-05883	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-130	Email from Ricks Tucker to Ray Hill	ATT-WIL-05888-5889	FRE 802 – Hearsay
PX-131	Email from Ryan Wager to Ray Hill; et al.	ATT-WIL-05897-5900	FRE 802 – Hearsay
PX-132	Email from Krissie Prebe to Ricks Tucker, Ray Hill	ATT-WIL-05902	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-133	Email from Ray Hill to James Jones	ATT-WIL-05908-5909	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-134	Email from Ray Hill to James Jones	ATT-WIL-05911-5912	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-135	Email from Ray Hill to Sherie Britain	ATT-WIL-05913-5914	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-136	Email from Ray Hill to Ryan Wager; et al.	ATT-WIL-05918-5919	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-137	Email from Sherie Britain to Ray Hill	ATT-WIL-05927	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-138	Meeting invite from Tony Le to "Tiger Team"	ATT-WIL-05947-5948	FRE 802 – Hearsay
PX-139	Email from Ray Hill to Mark Wirchniansky; et al.	ATT-WIL-05957-5958	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay
PX-140	Email from Ray Hill to Sherie Britain	ATT-WIL-05966-5967	FRE 407 – Subsequent remedial measures; FRE 802 – Hearsay

Exhibit No.	Description	Bates No. / Record Reference	Defendant's Objection(s)
PX-141	PART 1: AT&T Wireless Customer Agreement in effect March 2018–Nov. 2018 PART 2: AT&T Wireless Customer Agreement in effect Nov. 2018–Feb. 2019	ATT-WIL-05974-6016; ATT-WIL-01498-1537	No objection
PX-142	Excerpt of AT&T's Wireless Customer Agreement	ATT-WIL-05993-5994	FRE 106 – Incomplete; FRE 403 - Confuses issues
PX-143	Letter from AT&T to Mr. Williams	ATT-WIL-06116	FRE 802 Hearsay; FRE 407 Subsequent Remedial Measures
PX-144	Letter from AT&T to Mr. Williams	ATT-WIL-06117	FRE 802 Hearsay; FRE 407 Subsequent Remedial Measures

B. Defendant's Exhibits

Exhibit No.	Description	Bates No. / Record Reference	Plaintiff's Objection(s)
DX-1	AT&T Wireless Customer Agreement (Mar. - Nov. 2018)	ATT-WIL-05974-06016 (MSJ Ex. 3)	
DX-2	AT&T Wireless Customer Agreement (Nov. 2018 - Feb. 2019)	ATT-WIL-01498-01537 (MSJ Ex. 3)	
DX-3	Jason Williams' Signed Electronic Acknowledgement for AT&T Mobility Wireless Customer Agreement (2015-03-13)	ATT-WIL-01564 (MSJ Ex. 6)	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay
DX-4	Delaware Dept. of State - Entity Details re: Apollo Kids Mining, LLC	MSJ Ex. 7	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay
DX-5	2018 Hack Tracker (Notes by Plaintiff) (2018-19)	JW_0040-41 (Williams Dep. Ex. 2)	
DX-6	Data Activities Spreadsheet	JW_0089 (Williams Dep. Ex. 3)	
DX-7	Williams' communications with Gemini re: account (2018)	GEMINI_0009 (Williams Dep. Ex. 4)	

Exhibit No.	Description	Bates No. / Record Reference	Plaintiff's Objection(s)
DX-8	Expert Report of Ryan Garlick (2021-08-02)		
DX-9	Curriculum Vitae of Ryan Garlick	Garlick Ex. A	
DX-10	Antminer S9 Sold Auction Prices	Garlick Ex. B	
DX-11	List of materials reviewed by Garlick	Garlick Ex. C	
DX-12	"Actual vs. expected revenue," "Monthly Mining Profit with Proration" spreadsheet	Garlick Ex. D	
DX-13	Expenses & purchases analysis spreadsheet	Garlick Ex. E	
DX-14	Expert Report of Stephen Mott (2021-08-02)		
DX-15	Curriculum Vitae of Stephen Mott	Mott Ex. A	
DX-16	List of materials reviewed by Mott	Mott Ex. B	
DX-17	SIM Swaps Report	Mott Ex. C	
DX-18	Authentication for Activation and SIM Swaps	Mott Ex. D	
DX-19	Expert Report of Richard Sanders (2021-08-02)		
DX-20	Curriculum Vitae of Richard Sanders	Sanders Ex. A	
DX-21	Jason Williams' Social Media Posts	Sanders Ex. B	
DX-22	SIM Swapping Articles	Sanders Ex. C	
DX-23	DeHashed search results	Sanders Ex. D	
DX-24	Truthfinder Background Report on J. Williams (2021-01-23)	Sanders Ex. E	
DX-25	Rebuttal Report by Richard Sanders (2021-08-18)		
DX-26	Full graph of deposits to Gemini	Sanders Reb. Ex. A	
DX-27	Simple graph re: indirect transfers	Sanders Reb. Ex. B	

Exhibit No.	Description	Bates No. / Record Reference	Plaintiff's Objection(s)
DX-28	Spreadsheet of clustered addresses	Sanders Reb. Ex. C	
DX-29	Spreadsheet of clustered addresses	Sanders Reb. Ex. D	
DX-30	Oxt.me attribution	Sanders Reb. Ex. E	
DX-31	Slush Pool addresses	Sanders Reb. Ex. F	
DX-32	AT&T Account Notes for Jason Williams (2020-02-07)	ATT-WIL-00624-690 (Hill Dep. Ex. 4)	
DX-33	AT&T Doc: "What We've Done So Far for Hijack Prevention" (Dec. 2019)	ATT-WIL-04856-863 (Scheder Dep. Ex. 17)	
DX-34	Corrected Complaint (2019-10-25)	Dkt. 2	
DX-35	Plaintiff's Rule 26(a)(1) Initial Disclosures (2020-05-18)		
DX-36	Plaintiff's Responses & Objections to AT&T's First Set of Interrogatories (2020-07-06)		
DX-37	Plaintiff's 1st Supplemental Responses & Objections to AT&T's First Set of Interrogatories (2020-10-01)		
DX-38	Plaintiff's 2nd Supplemental Responses & Objections to AT&T's First Set of Interrogatories (2021-04-20)		
DX-39	Plaintiff's Responses & Objections to AT&T's Second Set of Interrogatories (2021-08-18)		
DX-40	Plaintiff's 1st Supplemental Responses & Objections to AT&T's Second Set of Interrogatories		

Exhibit No.	Description	Bates No. / Record Reference	Plaintiff's Objection(s)
	(2021-11-12)		
DX-41	Plaintiff's Responses and Objections to AT&T's First Set of Requests for Production (2020-07-03)		
DX-42	Plaintiff's Responses and Objections to AT&T's Second Set of Requests for Production (2021-02-08)		
DX-43	Plaintiff's Responses and Objections to AT&T's Third Set of Requests for Production (2021-08-13)		
DX-44	Plaintiff's Responses to AT&T's First Requests for Admission (2021-09-17)		
DX-45	AT&T's Rule 26(a)(1) Initial Disclosures (2020-05-18)		
DX-46	AT&T's First Amended Answer & Affirmative Defenses (2021-07-28)	Dkt. 79	
DX-47	Google Terms of Service – Privacy & Terms – updated October 25, 2017	ATT-WIL-07828-832	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay; FRCP 37 – Failure to Disclose in Discovery
DX-48	Jason Williams' November 2018 AT&T Account Invoice (2018-11-05)	ATT-WIL-07833-836	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay; FRCP 37 – Failure to Disclose in Discovery
DX-49	Jason Williams' December 2018 AT&T Account Invoice (2018-12-05)	ATT-WIL-07837-840	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay;

Exhibit No.	Description	Bates No. / Record Reference	Plaintiff's Objection(s)
			FRCP 37 – Failure to Disclose in Discovery
DX-50	Jason Williams' January 2019 AT&T Account Invoice (2019-01-05)	ATT-WIL-07841-844	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay; FRCP 37 – Failure to Disclose in Discovery
DX-51	Jason Williams' February 2019 AT&T Account Invoice (2019-02-05)	ATT-WIL-07845-848	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay; FRCP 37 – Failure to Disclose in Discovery
DX-52	Jason Williams' March 2019 AT&T Account Invoice (2019-03-05)	ATT-WIL-07849-852	FRE 401 – Relevance; FRE 901 – Authenticity; FRE 801-02 – Hearsay; FRCP 37 – Failure to Disclose in Discovery
DX-53	Deposition of Ray Hill (2021-11-17)		
DX-54	Deposition of Valerie Scheder (2021-11-30)		
DX-55	Deposition of Robert Arno (2022-02-28)		
DX-56	Deposition of Jason Williams (2022-02-23)		
DX-57	Appropriate demonstrative exhibits, to be determined		Plaintiff reserves the right to object to any demonstrative exhibits shown by Defendant

IV. DESIGNATION OF PLEADINGS AND DISCOVERY MATERIALS

A. Plaintiff's Designations

Description	Plaintiff's Designation(s)	Defendant's Objection(s)
Defendant's Answers and Objections to Plaintiff's First Set of Interrogatories, dated July 20, 2020	Interrogatories and Answers 1, 2, 3, 5, 7, 8, 12, 14; Interrogatory 10 and last paragraph of Answer 10	FRE 403 (Confuses issues and prejudicial effect outweighs probative value) FRE 611 (Attorney arguments).

Description	Plaintiff's Designation(s)	Defendant's Objection(s)
Defendant's Initial Disclosures Pursuant to F.R.C.P. 26(a)(1), dated May 18, 2020	Sections (i) and (ii)	FRE 403 (Confuses issues and prejudicial effect outweighs probative value); FRE 611 (Attorney arguments/reference to unverified discovery document); FRE 901 (Authentication).
Defendant's First Supplemental Initial Disclosures Pursuant to F.R.C.P. 26(a)(1), dated October 21, 2020	Entire	FRE 402, 403, prejudicial effect outweighs probative value); FRE 702 (Not disclosed as experts in this action); FRE 801-802, (Hearsay)
Defendant's Separate Statement of Undisputed Material Facts in Support of its Motion for Summary Judgment or Partial Summary Judgment in the Alternative (Doc. 127.3)	Paras. 8, 10	FRE 106 (Incomplete); FRE 801-802 (Hearsay - Previously filed under seal in this matter); FRE 403 (Prejudicial effect outweighs probative value); FRE 407 (Subsequent remedial measures).

B. Defendant's Designations

Description	Defendant's Designation(s)	Plaintiff's Objection(s)
Deposition of Jason Williams	5:4-17 53:1-58:18 63:8-64:19 86:2-90:10 77:11-25 200:15-201:5 254:4-255:12 275:16-24 306:1-5	FRCP 32(b) FRE 401, 402, 403 FRE 801, 802, 803 Plaintiff hereby incorporates his objection to the form of the questions in these portions of his deposition, as reflected in the transcript.
Plaintiff's Responses to AT&T's Requests for Admission	Williams' Responses to Request Nos. 8, 9, 13 and 23	FRE 106 FRE 401, 402, 403 FRE 801, 802, 803

Description	Defendant's Designation(s)	Plaintiff's Objection(s)
Plaintiff's Responses to Interrogatories	Williams' Responses to Interrogatories Nos. 4 and 10	FRE 106 FRE 401, 402, 403 FRE 801, 802, 803
Plaintiff's Supplemental Responses to Interrogatories	Williams' Supplemental Response to Interrogatory No. 5	FRE 106 FRE 401, 402, 403 FRE 801, 802, 803

V. WITNESSES

A. Plaintiff's Witnesses

Plaintiff intends to call the following witnesses in his case in chief. This summary is not intended to limit in any way the scope of such witnesses' testimony or Plaintiff's right to call additional witnesses as may be permitted by the Court for impeachment, rebuttal or other good cause.

1. Jason Williams (Plaintiff): Counsel will establish that Mr. Williams' AT&T phone was SIM swapped at least 6 times in a three-month period, and that he did not authorize any of those SIM swaps. Counsel will also establish the harms and damages suffered by Mr. Williams as result of the SIM swaps, including the loss of multiple online accounts (including cryptocurrency, email, and social media accounts), invasion of his privacy and security, and emotional damages.

2. Jameson Lopp (expert retained by Plaintiff): Counsel will establish the projected Bitcoin revenue that Mr. Williams would have earned from his mining operation if he had not been forced to shut it down as a result of the SIM swaps and resulting security breaches. Counsel will also establish that Mr. Williams'

steps to protect his online accounts were reasonable. To the extent AT&T's experts Ryan Garlick and Richard A. Sanders testify at trial, counsel will also establish that Mr. Lopp can offer rebuttal testimony with respect to those experts' anticipated opinions regarding Bitcoin revenue and online security measures, respectively.

3. Ray Hill (AT&T employee): Counsel will establish that Mr. Williams' AT&T phone was SIM swapped at least 6 times in a three-month period, and that he did not authorize any of those SIM swaps. Counsel will also establish that AT&T's security protocols for preventing Mr. Williams' SIM swaps were insufficient. Counsel will also establish AT&T failed to prevent the unauthorized access of Mr. Williams' CPNI.

4. Valerie Scheder (AT&T employee): Counsel will establish that AT&T's security protocols for preventing Mr. Williams' SIM swaps were insufficient. Counsel will also establish AT&T failed to prevent the unauthorized access of Mr. Williams' CPNI.

5. Robert Arno (AT&T employee): Counsel will establish that AT&T's security protocols for preventing Mr. Williams' SIM swaps were insufficient. Counsel will also establish AT&T failed to prevent the unauthorized access of Mr. Williams' CPNI.

B. Defendant's Witnesses

AT&T intends to call the following witnesses in its case in chief. This summary is not intended to limit in any way the scope of such witnesses' testimony or

AT&T's right to call additional witnesses as may be permitted by the Court for impeachment, rebuttal or other good cause.

1. Robert Arno: Mr. Arno is an AT&T employee. Mr. Arno is expected to testify as to Mr. Williams' AT&T account and AT&T's policies, procedures and response regarding SIM fraud.

2. Valerie Scheder: Ms. Scheder is an AT&T employee. Ms. Scheder is expected to testify as to AT&T's fraud management plans, tools, technology, policies and procedures, including AT&T's efforts and investments to combat SIM fraud.

3. Ray Hill: Mr. Hill is an AT&T employee. Mr. Hill is expected to testify as to AT&T's policies and procedures regarding SIM fraud, AT&T's response to SIM fraud, Mr. Williams' AT&T account, and AT&T's response to Mr. Williams' allegations of unauthorized SIM changes on his AT&T account.

4. Brian Rexroad. Mr. Rexroad is an AT&T employee. Mr. Rexroad is expected to testify as to AT&T's fraud management plans, tools, technology, policies and procedures, including AT&T's efforts and investments to combat SIM fraud.

5. Ryan Garlick: Mr. Garlick is an expert witness retained by AT&T. Mr. Garlick is expected to testify as to his opinions regarding the viability of Mr. Williams' cryptocurrency mining operations, and regarding Mr. Williams' claimed expenses, profits and losses regarding such operation, in accord with this expert report previously produced in this action.

6. Richard Sanders: Mr. Sanders is an expert witness retained by AT&T. Mr. Sanders is expected to testify as to his opinions regarding cryptocurrency, cryptocurrency mining, and the associated risks of holding and/or mining cryptocurrency. In connection with those opinions, in accord with his expert report and rebuttal expert report previously produced in this action, Mr. Sanders is also expected to testify as to his opinions regarding online criminal activity, Mr. Williams' online conduct and cybersecurity practices, including lack of damages and contributory negligence.

7. Stephen Mott: Mr. Mott is an expert witness retained by AT&T. Mr. Mott is expected to testify as to his opinions regarding the reasonableness of AT&T's policies and practices applicable to the prevention of unauthorized SIM changes and relevant industry standards, in accord with his expert report previously produced in this action.

8. Jason Williams: Mr. Williams is the Plaintiff in this action. AT&T intends to present Mr. Williams' testimony regarding his claims and AT&T defenses to such claims, including lack of damages and contributory negligence.

VI. ESTIMATE OF LENGTH OF TRIAL

The parties expect the trial to last 7 days.

VII. VERDICT FORMS

The parties' respective proposed verdict forms are attached hereto.

Dated: February 7, 2023

Respectfully submitted,

Counsel for Plaintiff:

/s/ Christopher LaVigne

Christopher LaVigne
Joseph Gallo
WITHERS BERGMAN LLP
430 Park Avenue
New York, New York 10022
Telephone: (212) 848-9800
Facsimile: (212) 848-9888
Christopher.LaVigne@withersworldwide.com
Joseph.Gallo@withersworldwide.com

/s/ Dhamian Blue

Dhamian Blue
205 Fayetteville Street
Suite 300
Raleigh, North Carolina 27601
Phone: (919) 833-1931
Fax: (919) 833-8009
dab@bluellp.com
State Bar No. 31405

Counsel for Defendant:

/s/ Joseph S. Dowdy

Joseph S. Dowdy (N.C. State Bar No. 31941)
KILPATRICK TOWNSEND & STOCKTON LLP
4208 Six Forks Road, Suite 1400
Raleigh, NC 27609
Telephone: (919) 420-1700
Facsimile: (919) 510-6120
Email: jdowdy@kilpatricktownsend.com

/s/ Nancy L. Stagg

Nancy L. Stagg (CA State Bar No. 157034)
KILPATRICK TOWNSEND & STOCKTON LLP
12255 El Camino Real, Suite 250
San Diego, CA 92130
Telephone: (858) 350-6156
Facsimile: (858) 350-6111
Email: nstagg@kilpatricktownsend.com

/s/ S. Mark Henkle

S. Mark Henkle
KILPATRICK TOWNSEND & STOCKTON LLP
1001 West Fourth Street
Winston-Salem, North Carolina 27101
Telephone: (336) 747-7531
Facsimile (336) 793-4876
Email: mhenkle@kilpatricktownsend.com

SO ORDERED this ___ day of February, 2023:

Robert T. Numbers, II
United States Magistrate Judge